Consumer Electronics Association
1919 South Eads Street
Arlington, VA
22202 USA
866-858-1555 toll free
703-907-7600 main
703-907-7601 fax
CE.org

January 27, 2015

Chairman Michael C. Burgess and Ranking Member Jan Schakowsky
House Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing, and Trade
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Burgess and Ranking Member Schakowsky;

The Consumer Electronics Association (CEA)® is the technology trade association representing the $223 billion U.S. consumer electronics industry. Every day, our more than 2,000 member companies are busy innovating; creating new technologies and American jobs. At CEA, we work to advance government policies that allow these companies to thrive.

In an increasingly digital world, data is the lifeblood of commerce. Stolen data also has value to criminals who appropriate it for identity theft and other crimes, and the black markets that permit such information exchange are sophisticated. It is difficult for consumers to protect themselves in this environment despite the best efforts of businesses to implement preventative cybersecurity measures. Unfortunately, the reality is that cybercriminals will find ways to breach computer networks even while businesses implement more and more sophisticated defenses.

Consumers and law enforcement agencies stand a much better chance of mitigating the consequences of cyber-theft if they have sufficient notification. To date, we have relied primarily on a patchwork of 47 different state data breach notification laws. These laws, while similar in effect, can have significantly different requirements related to notification timelines, content of consumer notices, and responsibilities to consumers in terms of identity theft mitigation. This system is confusing to consumers and presents daunting complications for businesses, including potentially conflicting requirements for notification to law enforcement. Furthermore, consumers could receive different information at different times because of this piecemeal approach, creating even more stress and confusion for the consumer. We need a single, preemptive federal data breach notification standard that will streamline the process of consumer and law enforcement notification. Consumers, law enforcement, and businesses alike will be given the certainty they need to effectively combat the harmful effects of stolen data.

Consumers should be able to count on a clear and consistent notification process. Congress needs to act to ensure consumers in one state get the same information, on the same timeline, as consumers in another. Businesses can better protect and inform their customers with one federal data breach notification standard that preempts the patchwork of state laws. Without preemption, a federal standard is just one more layer of confusion for businesses and consumers.

CEA supports federal preemption for a data breach notification standard, and thanks the Committee for holding a hearing on this key issue. We urge a bipartisan solution that will best serve consumers, law enforcement, and businesses in mitigating the harmful impact of stolen data. We stand ready to work with the Committee as it moves a legislative solution forward.

Sincerely,

Gary Shapiro
President and CEO